大通達甲（情管）第１号
平成２６年１月１７日

簿冊名	例規(１年)
保存期間	１　年

本部各課・所・隊・室長
警　察　学　校　長　殿
各　警　察　署　長

警　務　部　長

大分県警察情報セキュリティの管理体制に関する要綱の制定について（通達）

大分県警察情報システムの情報セキュリティの維持については、「大分県警察情報セキュリティ対策基準の改正について」（平成23年５月30日付け大通達甲（情管）第３号）により運用しているところであるが、情報セキュリティをめぐる情勢の変化を踏まえ、大分県警察情報セキュリティポリシーの体系を見直し、別添のとおり「大分県警察情報セキュリティの管理体制に関する要綱」を定め、本年４月１日から実施することとしたので、事務処理上誤りのないようにされたい。

なお、前記通達は、同日付けで廃止する。

(情報管理課指導・捜査支援係)
(情報管理課企画・運用・開発係)

別添

大分県警察情報セキュリティの管理体制に関する要綱

第１　総則

１　趣旨

この要綱は、大分県警察情報セキュリティ規程（平成16年大分県警察本部訓令甲第20号。以下「規程」という。）第５条第２項及び第８条の規定に基づき、大分県警察情報システム（以下「警察情報システム」という。）の情報セキュリティを確保するために必要な管理体制を定めるものとする。

２　用語の定義

この要綱における用語の意義は、それぞれ次のとおりとする。

(1)　大分県警察情報セキュリティポリシー

規程及び規程に基づいて定められた情報セキュリティに関する事項をいう。

(2)　入出力資料

警察情報システムに入力された又は警察情報システムにより出力された情報を記録した文書、図画及び電磁的記録（作成中のものを含む。）をいう。

(3)　ドキュメント

警察情報システムに関する次に掲げる文書、図画及び電磁的記録（作成中のものを含む。）をいう。

ア　システムドキュメント

(ｱ)　システム仕様書

(ｲ)　システム設計書（情報の処理手順並びに機器及びプログラムの構成の概要の記録をいう。）

(ｳ)　プログラム仕様書（情報の処理手順の概要の記録をいう。）

(ｴ)　プログラムリスト

(ｵ)　操作指示書（システムの維持管理に伴う機器の設定方法等を説明した記録をいう。）

イ　取扱説明書

システムを利用する者が業務を行う上で参照する機器の操作の方法を説明した記録をいう。

(4)　外部記録媒体

磁気テープ、フラッシュメモリ、ＤＶＤ規格媒体等電子計算機に接続し、情報を入出力する電磁的記録媒体をいう。

(5)　情報

入出力資料、ドキュメント及び外部記録媒体又は警察情報システム内部に記録された情報をいう。

(6)　ネットワーク機器

警察情報システムを構成するルータ、ハブ等の機器又はこれらから出力されるデー

タを利用することによりネットワークを管理する機能を有する機器をいう。

(7) モバイル端末

一の警察の庁舎内から移動して運用するものとして整備した電子計算機（携帯電話機（スマートフォンを含む。）を含む。）をいう。

(8) サーバ等

情報を体系的に記録し、検索し、又は編集する機能を有するサーバ及びメインフレームをいう。

第２ 区域情報セキュリティ管理者

１ 区域情報セキュリティ管理者の設置

(1) 警察本部の庁舎の敷地を次に掲げる区域に分類する。

ア クラスＡ 各庁舎の敷地内であって、職員以外の者が自由に立ち入ることのできる区域

イ クラスＢ 執務室

ウ クラスＣ 警察情報システムに係る機械室

(2) クラスＢ及びクラスＣの区域に区域情報セキュリティ管理者を置き、それぞれ次に掲げる者をもって充てる。

ア クラスＢの区域 各所属の長（警察本部の課（所及び隊を含む。）の分室等で庁舎を別にするときは、警部（同相当職を含む。以下同じ。）以上の職員の中から当該所属の長が指名するもの）

イ クラスＣの区域 機械室を管理する所属の長（当該機械室が執務室と庁舎を別にする場所にあるときは、警部以上の職員の中から当該所属の長が指名するもの）

２ 区域情報セキュリティ管理者の任務

区域情報セキュリティ管理者は、当該区域における情報セキュリティの確保のための管理対策を行う。

３ 区域情報セキュリティ管理者の遵守事項

区域情報セキュリティ管理者は、関係する他の区域情報セキュリティ管理者、情報セキュリティ管理者等と連携し、次に掲げる対策を実施すること。

(1) クラスＢの区域の管理対策

ア クラスＡの区域との境界を施錠可能な扉等によって仕切ること。

イ 無人となるときは施錠すること。

ウ 情報セキュリティ管理者が認めた場合を除き、職員とそれ以外の者を視覚上区別できるようにすること。

エ 職員以外の者を立ち入らせるときは、入室用件等を確認すること。

オ 職員以外の者を立ち入らせるときは、当該区域内に設置された電子計算機の画面を不正に視認されないよう留意すること。

(2) クラスＣの区域の管理対策

ア 常時施錠し、立ち入ることができる者の名簿を作成すること。ただし、名簿に記

載された者以外の者を立ち入らせるときは、区域情報セキュリティ管理者の承認を得ること。

イ　当該区域に立ち入る者の氏名及びその入退室の時刻を記録すること。当該記録は、可能な限り電磁的に記録すること。

ウ　電子計算機の画面、システムドキュメント及び入出力資料をその区域の外から視認することができない構造とすること。

エ　職員以外の者を立ち入らせている間は、職員が立ち会うこと。ただし、当該区域に設置されたサーバ等の保守点検及び開発作業のため当該区域に常駐する目的で保守契約業者から派遣された者を立ち入らせる場合は、この限りでない。

オ　自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策を講ずること。

4　例外

情報セキュリティ管理者が、前記１(1)の分類による運用を困難と認めたときは、当該分類によらない区域を設けることができる。この場合において、情報セキュリティ管理者は、前記３の規定を参考として、可能な限り情報セキュリティの確保のための管理対策を行うこと。

第３　システムセキュリティ管理者

1　システムセキュリティ管理者の設置

大分県警察にシステムセキュリティ管理者を置き、警務部情報管理課長をもって充てる。

2　システムセキュリティ管理者の任務

システムセキュリティ管理者は、情報セキュリティ管理者を補佐する。

第４　システムセキュリティ責任者

1　システムセキュリティ責任者の設置

警察情報システムの整備を担当し、警察情報システムを構成する電子計算機及びネットワーク機器の管理者権限を保有する所属にシステムセキュリティ責任者を置き、当該所属の長をもって充てる。

2　システムセキュリティ責任者の任務

システムセキュリティ責任者は、次に掲げる事務を処理する。

(1)　整備する警察情報システムが必要な情報セキュリティ要件を備えるための事務

(2)　担当する警察情報システムの維持管理のための事務

3　システムセキュリティ責任者の遵守事項

(1)　システムセキュリティ責任者は、整備する警察情報システムの情報セキュリティ要件について、あらかじめ情報セキュリティ管理者の確認を受けること。

(2)　システムセキュリティ責任者は、警察情報システムを利用する業務の主管課の長と連携の上、当該システムの運用要領を策定するなどして、職員が当該システムを取り扱う際に遵守すべき事項を職員に周知するとともに、情報セキュリティ管理者に通知

すること。遵守すべき事項には、次に掲げる事項を含めること。

ア　当該システムにおいて取り扱うことのできる情報の機密性の分類の範囲

イ　当該システムにおいて、職員が独自の判断で行うことのできる改造（新たな機器の接続、ソフトウェア追加等）の範囲

(3)　システムセキュリティ責任者は、所管する警察情報システムについて、情報セキュリティに係る脆弱性に関する情報（以下「脆弱性情報」という。）を入手したときは、情報セキュリティ管理者に報告するとともに、当該脆弱性情報が警察情報システムにもたらすリスクを分析した上で、対策を講ずること。

(4)　システムセキュリティ責任者は、警察情報システムについて、災害時等においても継続して運用できるよう十分検討し、必要に応じて業務継続計画を策定すること。また、当該業務継続計画は、可能な限り情報セキュリティポリシーとの整合を図ること。

(5)　システムセキュリティ責任者は、警察情報システムの情報セキュリティ対策について見直しを行う必要性の有無を適宜検討し、必要があると認めた場合にはその見直しを行い、必要な措置を執ること。

(6)　システムセキュリティ責任者は、管理者権限を適正に運用すること。

(7)　システムセキュリティ責任者は、各種ソフトウェアのうち利用しない機能は無効化すること。

(8)　システムセキュリティ責任者は、定期的に脆弱性情報に係る対策及び導入したソフトウェアのバージョンアップ等の状況を記録し、これを確認・分析するとともに、不適切な状態にある電子計算機及びネットワーク機器を把握したときには適切に対処すること。

(9)　システムセキュリティ責任者は、大分県警察情報セキュリティポリシー等に違反する行為を認知したときは、速やかにシステムセキュリティ管理者に報告すること。

第５　運用管理者等

１　運用管理者の設置

警察情報システムを運用する所属に運用管理者を置き、当該所属の長をもって充てる。

２　運用管理者の任務

運用管理者は、所属における警察情報システムの運用に関し、情報セキュリティの維持その他の警察情報システムによる処理に係る情報の適正な取扱いを確保するために必要な事務を処理する。

３　運用管理補助者の設置

前記１の所属に運用管理補助者を置き、警察本部にあっては次席、副所長及び副隊長を、警察学校にあっては副校長を、警察署にあっては副署長をもって充てる。

４　運用管理補助者の任務

運用管理補助者は、運用管理者の事務を補助する。

第６　システム管理担当者

１　システム管理担当者の設置

システムセキュリティ責任者は、その管理するシステムごとにシステム管理担当者を指名し、業務の責務に即した必要な範囲において、管理者権限を付与すること。

2　システム管理担当者の任務

システム管理担当者は、担当する警察情報システムに係るシステム管理に関する業務を行う。

3　システム管理担当者の遵守事項

(1)　システム管理担当者は、権限のない者にＩＤを発行しないこと。

(2)　システム管理担当者は、警察情報システムに係るドキュメントを適正に管理すること。

(3)　システム管理担当者は、管理対象となる電子計算機に関連する脆弱性情報の入手に努めること。情報を入手したときは、システムセキュリティ管理者及びシステムセキュリティ責任者に報告すること。

(4)　システム管理担当者は、クラスＣの区域に設置されている警察情報システムを構成する機器、外部記録媒体及びシステムドキュメントを、クラスＢ以下の区域に持ち出すときは、その状況を記録すること。

(5)　システム管理担当者は、システムの構成の変更等の作業（軽微なものを除く。）を行う場合において、情報セキュリティの観点から、あらかじめその影響を確認するとともに、その作業を監視し、必要な対応を行うこと。

第７　ネットワーク管理担当者

1　ネットワーク管理担当者の設置

システムセキュリティ管理者は、その管理するネットワークごとにネットワーク管理担当者を指名し、業務の責務に即した必要な範囲において、管理者権限を付与すること。

2　ネットワーク管理担当者の任務

ネットワーク管理担当者は、担当するネットワーク機器に係るネットワーク管理に関する業務を行う。

3　ネットワーク管理担当者の遵守事項

(1)　ネットワーク管理担当者は、管理対象となるネットワーク機器に関連する脆弱性情報の入手に努めること。情報を入手したときは、システムセキュリティ責任者に報告すること。

(2)　ネットワーク管理担当者は、担当するネットワーク機器について、データ伝送に関する監視及び制御を行うこと。

(3)　ネットワーク管理担当者は、担当するネットワークの構成の変更等の作業（軽微なものを除く。）を行う場合において、情報セキュリティの観点から、あらかじめその影響を確認するとともに、その作業を監視し、必要な対応を行うこと。

第８　運用管理担当者

1　運用管理担当者の設置

(1)　モバイル端末及び外部記録媒体を利用する所属に一人又は複数人の運用管理担当者

を置き、運用管理者が指名する者をもって充てる。

⑵　運用管理担当者は、警部以上の職員とする。ただし、やむを得ない事情がある場合は、この限りでない。

2　運用管理担当者の任務

運用管理担当者は、モバイル端末の保管及び利用状況の管理、外部記録媒体の保管並びに外部記録媒体を利用した情報の入出力の管理に係る事務を行う。

第9　その他

1　台帳の整備

情報セキュリティ管理者は､警察情報システムについて一元的に把握し管理するため、必要な事項を記載した台帳を整備すること。

2　大分県警察情報セキュリティポリシーに係る教養

情報セキュリティ管理者は、職員に大分県警察情報セキュリティポリシーを正しく理解させ、確実に遵守させるため、職員に対し、職務に応じた教養を実施すること。

3　災害時等における措置

情報セキュリティ管理者は、災害時等において、警察情報システムの復旧、通信手段の確保等のためにやむを得ないときは、大分県警察情報セキュリティポリシーの規定にかかわらず、所要の措置を執ること。

4　情報セキュリティインシデント発生時の措置

不正プログラム感染等の情報セキュリティインシデントが発生した際の措置については、情報セキュリティ管理者が別に定める。

5　大分県警察情報セキュリティポリシーの見直し

大分県警察情報セキュリティポリシーの規定については、見直しを行う必要性の有無を適宜検討し、必要があると認めた場合にはその見直しを行うこと。

附　則

この要綱は、平成26年４月１日から施行する。